BOBBY JINDAL
GOVERNOR

ANGELE DAVIS
COMMISSIONER OF ADMINISTRATION

State of Louisiana

Division of Administration
OIT Enterprise Security Office

MONTHLY SECURITY TIPS

August 2008

Security Concerns – Peer to Peer (P2P) File Sharing

Security Concerns Regarding Peer To Peer (P2P) File Sharing

Peer-to-Peer (P2P) networking has become a popular method for sharing files, music, photographs and other information. P2P allows computer users, utilizing the same P2P software, to connect with each other and directly access files from one another's hard drives.

Although the concept of file sharing seems benign, there are a number of risks associated with P2P.

Some of the major risks are:

- ✓ Sharing files on your computer with anonymous and unknown users on the Internet is contrary to the basic principles of securing your computer.
- ✓ Even if you know the source, in P2P, opening a file has risks – it may contain a Trojan horse, worm, virus or other malware.
- ✓ P2P may expose personal, private or confidential data on your computer.
- ✓ P2P software, like any other application, may contain vulnerabilities which could allow unauthorized access.
- ✓ It is possible that the P2P software may be a malicious version - it might include a virus or Trojan.
- ✓ In order to share files on your computer or to access files on other computers within a P2P network, you generally must authorize access through your firewall. This exposes your system to potentially malicious traffic from the Internet that otherwise may have been blocked by the firewall.
- ✓ P2P traffic may consume your bandwidth, diminish your computer's performance, cause a denial of service and impede access to the Internet.
- ✓ Some P2P programs may implement default settings that you do not want to use, such as scanning your entire drive, looking for files to share.
- ✓ Some of the files shared or downloaded may include copyrighted material, pirated software and other illegal material

Because the negative effects of P2P far outweigh any potential benefits, the best way to protect your computer/system is to avoid P2P technology.

Installation of malicious code - When you use P2P applications, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected.

Michael Gusky, Chief Information Security Officer
Tel: (225) 219-9475 • Cell: (225) 247-6588 • Mike.Gusky@la.gov

Exposure of sensitive or personal information - By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.

Susceptibility to attack - Some P2P applications may ask you to open certain ports on your firewall to transmit the files. However, opening some of these ports may give attackers access to your computer or enable them to attack your computer by taking advantage of any vulnerabilities that may exist in the P2P application. There are some P2P applications that can modify and penetrate firewalls themselves, without your knowledge.

Denial of service - Downloading files causes a significant amount of traffic over the network. This activity may reduce the availability of certain programs on your computer or may limit your access to the internet.

Copyright Law and the Risk of Prosecution - Files shared through P2P applications may include pirated software, copyrighted material, or pornography. If you download these, even unknowingly, you may be faced with fines or other legal action.

Online Resources

How To Disable Various P2P Software On Your Computer
http://security.uchicago.edu/guidelines/peer-to-peer/

Good and Bad Executable File Extensions
http://www.novatone.net/mag/mailsec.htm

Tips To Avoid Problems With P2P File Sharing
http://netsecurity.about.com/od/newsandeditorial1/a/p2psecurity.htm

P2P File Sharing Tips
http://onguardonline.gov/p2p.html

The information provided in this Monthly Security Tips Newsletter is intended to increase the security awareness of end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the State's overall cyber security posture

Michael Gusky, Chief Information Security Officer
Tel: (225) 219-9475 • Cell: (225) 247-6588 • Mike.Gusky@la.gov